FGT5006.003 DNS Manipulation: Poisoning

DNS Security Problem Statement

1 Introduction

5G SA roaming will need SEPP discovery mechanisms that require DNS resolution between operators, so DNS security is becoming more important. The scope is the internal IPX DNS. There is increased need for on DNS security (authentication and integrity). The new 5G use cases may increase the business case for MNO investment in DNS security.

2 Problem statement

The internal DNS of the IPX eco system makes use of an unsecured form of DNS. This means that connections as well as records are not secured (authentication, integrity protection and encryption). Not securing DNS could lead to attacks against networks (e.g. DNS poisoning) and/or customers (e.g. DNS request/response interception).

In 5G, more crucial services are built on the IPX ecosystem, most notably discovery of SEPPs via NAPTR and SRV records.

Unlike the Internet DNS, for the IPX network the focus does not lie on encryption of DNS traffic. Instead, the DNS ecosystem IPX network for the internal DNS could become subject to DNS poisoning attacks and therefore the potential work should focus on authentication and integrity of the records and the entire DNS chain.

3 Call for action

GSMA members should collaborate within and between the relevant working groups (DESS, IG, FSAG etc.) to study and develop recommendations on the following items:

- Is DNSSEC the best solution to address the problem outlined above?

- Is DNSSEC feasible to accomplish in the entire chain? (Political, financial, technical)

- If yes, how to get the DNS ecosystem within the IPX ecosystem moving towards implementation?

- Are there other options to add more security to the IPX DNS, and in particular to reduce the risk of DNS poisoning?

- Shall we take security to the end points into account as part of this action?

Description: An adversary can hide user traffic within DNS requests that are part of the data sessions and transmit data undetected.

An adversary can hide user within DNS requests that are part of data sessions to access the Internet and transmit data undetected. This can be used for redirecting users via adversary in the middle attacks and to hide traffic for billing fraud, command and control of a bot or other device, or for any other task where hidden traffic is useful.

Labelling:

* Sub-Technique(s): N/A
* Applicable Tactics: Fraud, Command and Control, Exfiltration

Metadata:

* Architecture segment: User plane, Control plane.
* Platforms: 5G
* Access type required: user
* Data Sources: Network Traffic
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Free fake DNS loophole | Operators do not enforce free DNS service via the standard five-tuple flow ID (src IP, dest IP, src port, dest port, protocol). Instead, they use only the destination port (or plus protocol ID), thus exposing an obvious vulnerability. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGM1557 | Use strong data integrity protection algorithms |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unauthenticated DNS Services | The end user must not have the capability to validate whether it is communicating with a malicious DNS or a valid one. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| DNS Servers | Whoever controls the DNS Servers controls how and what end users connect to over the network, making DNS Servers a type of critical infrastructure. |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0029 | Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP) |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Billing Fraud | Attacker will be able to route traffic through DNS channels to use the network free of charge. |
| Command and Control Network | Attacker can route command and control traffic through DNS to control botnets or other entities. |
| Exfiltration Route | Attacker has a route to exfiltrate stolen data disguised as DNS packets. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| “Badhra Framework”: S.P. Rao, S. Holtmanns, T. Aura, “Threat modeling framework for mobile communication systems” | https://arxiv.org/pdf/2005.05110.pdf |
| Mobile Data Charging: New Attacks and Countermeasures | https://dl.acm.org/doi/pdf/10.1145/2382196.2382220 |
| Merve Sahin, Aurelien Francillon, Payas Gupta, and Mustaque Ahamad. 2017.  “*Sok: Fraud in telephony networks*”. In 2017 IEEE European Symposium on Security  and Privacy (EuroS&P). IEEE, p235–250 | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7961983&tag=1 |
| Kui Xu, Patrick Butler, Sudip Saha, Danfeng (Daphni) Yao in DNS CC Journal, “DNS for Massive-Scale Command and Control” | https://people.cs.vt.edu/~danfeng/papers/DNS-CC-JOURNAL.pdf |